SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

I documenti allegati sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 18 JUNI 2003

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

H. Jenni

Heinz Jenni

Protecting Intellectual Property

Demande de brevet no 2002 1403/02

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Méthode de vérification de la validité d'une clé pour un réseau domestique numérique.

Requérant:
Nagravision S.A.
22, Route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire:
Leman Consulting S.A.
62, route de Clémenty
1260 Nyon

Date du dépôt: 19.08.2002

Classement provisoire: H04L, H04N

MÉTHODE DE VÉRIFICATION DE LA VALIDITÉ D'UNE CLÉ POUR UN RÉSEAU DOMESTIQUE NUMÉRIQUE

La présente invention concerne une méthode de sécurisation dans un réseau domestique numérique. Plus particulièrement, la méthode de l'invention s'articule sur des réseaux uniques d'appareils dont les contenus sont personnalisés.

Un réseau domestique numérique est un ensemble d'appareils audio-visuels reliés par des interfaces numériques. Ces appareils incluent par exemple des décodeurs numériques, téléviseurs numériques, lecteurs / enregistreurs de DVD, appareils de stockage munis de disques durs, enregistreurs audio MP3, des livres électroniques, consoles de jeux, ordinateurs ou autres plate-formes permettant l'accès à Internet.

La technologie numérique donne la possibilité d'effectuer des copies de contenus (films, musique, jeux vidéos, logiciels...) qui sont de même qualité que l'original. Ces copies parfaites impliquent des conséquences néfastes pour l'industrie au niveau des droits d'auteurs si une protection efficace n'est pas disponible.

Le contenu original arrive dans la maison par diverses sources: il peut être transmis par voie hertzienne, par le satellite ou le câble, par l'Internet, ou être enregistré sur une cassette numérique, un DVD ou même un disque dur. Avant de fournir leur contenu aux distributeurs, les détenteurs des droits spécifient certaines conditions d'accès concernant la protection du contenu et doivent donc être mises en vigueur par un système de protection du contenu à l'intérieur de la maison.

Un contenu peut, par exemple, être associé à des droits comme: "Lecture seule", "Copie pour usage privé", "Copie libre".

Un système de protection des contenus numérique va permettre aux propriétaires et distributeurs de contenus de lutter contre les pertes de revenus dues au piratage. Il est basé sur l'utilisation de modules de sécurité permettant une identification de chaque appareil connecté sur le réseau domestique et le décodage des données.

L'avantage d'un tel système est que le contenu est toujours conservé crypté dans le réseau numérique domestique jusqu'à ce qu'il soit lu. Le décryptage est réalisé en collaboration avec le module de sécurité amovible inséré dans l'appareil de lecture. Cette méthode simple offre une sécurité complète de l'encryptage.

Un tel système de protection est qualifié de "bout en bout", c'est-à-dire depuis l'entrée du contenu sur le réseau domestique numérique jusqu'à sa restitution, en passant par son stockage éventuel.

Avec ce système, les fournisseurs de contenus peuvent facilement choisir des droits pour les utilisateurs de données encryptées qui seront appliqués au réseau domestique.

Une possibilité de dupliquer et de gérer des contenus numériques à l'intérieur de son réseau est ainsi offerte à l'utilisateur dans le cadre des droits définis par les fournisseurs de contenus. Elle permet à l'utilisateur de partager le contenu enregistré sur n'importe quel appareil numérique fixe ou portable connecté, tout en empêchant la redistribution de ce contenu à l'extérieur de son réseau personnel.

Le système crée un environnement sécurisé: il permet d'enregistrer des contenus cryptés, mais en interdit la lecture si le contenu n'est pas légitime. Un contenu illégitime est une copie non autorisée par le détenteur des droits associés. Par exemple, un disque copié à partir d'un original sur un appareil appartenant à un réseau A ne pourra pas être lu par un appareil connecté à un réseau B.

Tout contenu non gratuit est associé à un réseau domestique donné et, par conséquent, ne peut être utilisé que sur ce même réseau. L'identité au réseau est assurée par les modules de sécurité qui, du fait qu'ils sont amovibles, permettent une certaine mobilité.

Cependant, un réseau domestique peut également comprendre des appareils mobiles externes associés à ce réseau, par exemple un lecteur de musique portable ou un appareil dans une voiture, ainsi que des appareils dans une résidence secondaire qui appartient au propriétaire du réseau initial. Autrement dit, les contenus sont protégés par la même clé dès que les appareils externes ont été connectés au moins une fois au réseau de référence. Il n'est donc pas nécessaire d'avoir une connexion permanente. Tous ces appareils partagent une clé propre à un réseau privé domestique, sur lequel le contenu est disponible pour un usage privé, mais seulement selon les droits associés.

Le système de protection dont les principes sont évoqués ci-dessus est décrit dans le document de Thomson Multimedia SA: "SmartRight™, A Content Protection System for Digital Home Networks, White Paper" publié en octobre 2001.

Selon une configuration particulière, le point d'entrée d'un réseau domestique numérique est constitué d'un décodeur ("Set-Top-Box") qui reçoit un flux de données crypté à partir d'un satellite, d'un câble, voire par le biais d'Internet. Ce décodeur est muni d'un module de sécurité en général sous forme d'une carte à puce appelée carte convertisseur. Le rôle de cette carte consiste à traiter les conditions définies par le contrôle d'accès du fournisseur d'accès conditionnel donc à décrypter les messages de contrôle (ECM) contenant les mots de contrôle (CW) permettant le déchiffrement du contenu si les droits sont présents dans cette carte. Dans l'affirmative, cette carte réencrypte les mots de contrôle (CW) grâce à une clé de session générée aléatoirement par la carte. Cette carte joint aux mots de contrôle (CW) la clé de session encryptée par la clé de réseau pour former des messages de contrôle locaux (LECM).

La clé de réseau est une clé propre à un réseau donné. Elle est générée dans le réseau au moyen d'un module de sécurité en général sous forme d'une carte à puce appelée carte de terminal associée au premier appareil de visualisation du contenu se connectant au réseau. Ce dernier module est le seul capable d'initialiser le réseau. Un module terminal additionnel reçoit ensuite la clé de réseau de la part du premier appareil.

Par contre, la clé de réseau n'est pas connue de la carte convertisseur afin d'éviter d'y concentrer tous les secrets, ce qui en ferait une cible privilégiée d'attaque pour les pirates. Par conséquent, un mécanisme de communication sécurisé doit être mis en place entre une carte de terminal et la carte convertisseur pour que cette dernière puisse insérer la clé de session encryptée par la clé de réseau dans les messages de contrôle (LECM) qu'elle génère.

A cette fin, la carte de terminal échange avec la carte convertisseur une clé publique connue de la carte de terminal et une clé de session générée aléatoirement par la carte convertisseur. La carte de terminal transmet sa clé publique à la carte convertisseur qui retourne la clé de session cryptée avec la clé publique. La carte de

terminal décrypte alors la clé de session, puis retransmet à la carte convertisseur cette clé de session cryptée avec la clé de réseau.

La carte convertisseur encrypte d'une part les mots de contrôle (CW) à l'aide de la clé de session et d'autre part, elle y joint la clé de session cryptée avec la clé de réseau (provenant d'une des cartes de terminal) pour former les messages de contrôle locaux (LECM). Ces messages (LECM) sont alors transmis avec le contenu crypté aux différents appareils du réseau pour stockage ou visualisation.

Chaque appareil terminal connecté au réseau peut donc décrypter les messages (LECM) et en extraire les mots de contrôle (CW) car il possède la clé de réseau et il reçoit la clé de session cryptée par la clé de réseau. Il peur ensuite, à l'aide de ces mots de contrôle (CW), décrypter le flux de données.

Ce procédé d'introduction d'une clé de réseau contenue dans une carte terminal présente un inconvénient par le fait qu'il est techniquement possible d'initialiser une multitude de réseaux domestiques au moyen d'une carte de terminal falsifiée. En effet, dans le système de protection connu, la clé de réseau n'est pas contenue en tant que telle dans la carte convertisseur, mais seulement sous la forme d'une clé de session cryptée par la clé de réseau. Des réseaux non autorisés ainsi établis peuvent posséder donc tous la même clé et par conséquent, les contenus enregistrés dans les appareils peuvent être redistribués et exploités en dehors du nombre limité de membres tels que défini dans la norme d'un réseau domestique.

De plus, une clé de réseau tierce non reconnue par le fournisseur de contenu peut être introduite dans une carte de terminal permettant la création d'un réseau dont les droits attribués aux contenus ne sont plus gérés par le détenteur.

Le but de la présente invention est de pallier les inconvénients décrits ci-dessus en proposant une méthode de contrôle de la conformité de la clé de réseau.

Le but est atteint par méthode de vérification de la validité d'une clé de réseau dans un réseau domestique numérique comprenant un décodeur de flux de données encryptées par des mots de contrôle qui sont eux-mêmes contenus dans des messages de contrôle (ECM) provenant d'un centre de gestion et un ou une pluralité d'appareils définissant un réseau domestique, ledit décodeur comportant un module

de sécurité appelé carte convertisseur chargée de réencrypter les mots de contrôle avec une clé de session générée aléatoirement par ladite carte formant des messages de contrôle locaux (LECM), ledit réseau partageant une clé de réseau propre au dit réseau et stockée uniquement dans les modules de sécurité des appareils de visualisation appelés cartes de terminal, la clé de session accompagnant lesdits messages de contrôle locaux (LECM) étant encryptée par la clé de réseau dans une des cartes de terminal, caractérisée par les étapes suivantes:

- réception par la carte convertisseur d'une clé de test et de données de contrôle provenant du centre de gestion via le décodeur,

- transmission de la clé de test via le réseau domestique vers une carte de terminal associée à l'un des appareils connectés au réseau,

- encryption par la carte de terminal de la clé de test avec la clé de réseau contenue dans ladite carte de terminal,

- transmission de la clé de test encryptée vers la carte convertisseur,

- comparaison de la clé de test encryptée avec les données de contrôle précédemment reçues,

- acceptation ou refus de transmettre des données à ce réseau domestique en fonction du résultat de la comparaison.

La méthode s'applique généralement lors de transfert de données provenant d'une source à accès conditionnel vers un réseau domestique. Il s'agit de vérifier l'authenticité d'une clé de réseau par l'intermédiaire de données de contrôle pertinentes fournies par le centre de gestion en général sous forme d'une liste.

La méthode est basée sur la vérification de la présence ou de l'absence d'un cryptogramme donné sur une liste de contrôle: le cryptogramme étant constitué à partir d'une clé de test fournie par le centre de gestion encryptée un module de sécurité d'un appareil connecté au réseau à l'aide d'une clé de réseau.

La liste de contrôle fournie par le centre de gestion contient des cryptogrammes créés soit avec des clés de réseau invalides ("black list"), soit avec des clés valides ("white list"). Une clé de réseau contenue dans une carte de terminal sera donc

valide seulement si son cryptogramme correspondant est absent d'une "black list" ou présent dans une "white list".

Une clé de réseau reconnue comme valide permet la génération d'une clé de session par la carte convertisseur du décodeur, clé qui sera transmise de manière sécurisée à la carte de terminal d'un des appareils. Cette clé de session est alors encryptée par la clé de réseau de la carte de terminal. La carte convertisseur transmet la valeur résultante avec les mots de contrôle (CW) encryptés par la clé de session.

Dans la négative, la carte convertisseur stoppe la génération du flux de données de contrôle accompagnant le contenu et permettant son déchiffrement au sein du réseau domestique. Un message d'erreur invite l'utilisateur à changer de carte de terminal. Dans une variante où le décodeur possède un canal de retour, ce message peut être aussi transmis au centre de gestion pour signaler une carte de terminal non valide.

Selon cette méthode la clé de session est remplacée dans une phase de test, par une clé de test à valeur prédéfinie reçue du centre de gestion. La clé de test joue alors un rôle analogue à celui de la clé de session du procédé d'initialisation décrit plus haut.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux figures annexées servant d'exemple nullement limitatif, à savoir:

La figure 1 représente une communication typique entre une carte de terminal et une carte convertisseur selon la méthode de l'état de la technique.

La figure 2 représente une communication typique entre une carte de terminal et une carte convertisseur selon la méthode de l'invention.

Le réseau domestique numérique illustré par la figure 1 est composé d'un décodeur (STB), des téléviseurs (TV1, TV2) et d'un ordinateur (PC). Chaque appareil est muni d'une carte à puce amovible servant de module de sécurité chargé de l'encryptage / décryptage des données du réseau. Selon une variante particulière, le module de la carte à puce peut être directement monté dans l'appareil de manière permanente.

Selon une réalisation préférée, la carte associée au décodeur (STB) est une carte convertisseur (CC) qui transforme des messages de contrôles ECM (Entitlement Control Message) reçus par le décodeur en ECM locaux (LECM) propres au réseau. Ces derniers contiennent les clés de décryptage ou mots de contrôle (CW) du flux de données (DT) provenant du centre gestion encryptés par une clé de session (SK). Les ECM locaux (LECM) contiennent aussi cette clé de session encryptée par la clé de réseau (NK).

Les cartes associées aux appareils de visualisation (TV1, TV2, PC) appartenant au réseau sont des cartes de terminal (CT) qui permettent le décryptage des données du réseau au niveau des appareils (TV1, TV2, PC) grâce à la clé de réseau (NK) stockée dans chacune d'elles.

La liaison entre un réseau à accès conditionnel et un réseau domestique s'effectue par la connexion d'un appareil par exemple (TV1) au décodeur (STB). Lorsque la carte convertisseur (CC) associée au décodeur (STB) doit transformer des messages de contrôles ECM (Entitlement Control Message) en des ECM locaux (LECM) propres au réseau, un dialogue s'établit entre la carte de terminal (CT) associée à l'appareil (TV1) et la carte convertisseur (CC). Ce dialogue s'effectue de manière sécurisée en utilisant une paire de clés asymétriques (clé publique et clé privée) propre à la carte de terminal (CT); il se résume en 3 étapes (1, 2, 3) comme suit:

1).- La carte de terminal du premier appareil transmet sa clé publique (PK) à la carte convertisseur (CC) du décodeur (STB).

2).- La carte convertisseur (CC) génère aléatoirement une clé de session (SK) qu'elle crypte avec la clé publique (PK) précédemment reçue. La carte convertisseur (CC) transmet alors la clé encryptée $(SK)_{PK}$ à la carte de terminal (CT).

3).- La carte de terminal (CT) décrypte la clé de session (SK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de session (SK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le message résultant $(SK)_{NK}$ est transmis à la carte convertisseur (CC).

Les messages de contrôle locaux (LECM) comprennent finalement des mots de contrôle (CW) encryptés par une clé de session (SK) et cette clé (SK) encryptée par la clé de réseau (NK).

Le téléviseur (TV1) muni de sa carte de terminal (CT) est alors capable de décrypter les messages de contrôle locaux (LECM) grâce à la clé de réseau (NK) qui sert à décrypter la clé de session (SK). Cette dernière permet ensuite la décryption de mots de contrôle (CW) servant à décrypter les données vidéo / audio destinées au téléviseur.

La figure 2 illustre le procédé d'initialisation de la communication selon l'invention dont les étapes se différencient par rapport aux précédentes par le fait que la clé de session (SK) est remplacée, dans une première phase, par une clé de test (TK) provenant du centre de gestion. Ce dernier transmet en plus de la clé de test (TK) une liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$:

1).- La carte de terminal (CT) du premier appareil transmet sa clé publique (PK) à la carte convertisseur (CC) du décodeur (STB).

2).- La carte convertisseur (CC) reçoit de la part du centre de gestion une liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ ainsi qu'une clé de test (TK). La carte convertisseur (CC) crypte la clé de test (TK) avec la clé publique (PK) reçue de la carte de terminal (CT), ce qui donne un nouveau message $(TK)_{PK}$ qui sera retransmis à la carte de terminal (CT).

3).- La carte de terminal (CT) décrypte la clé de test (TK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de test (TK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le cryptogramme résultant $(TK)_{NK}$ est transmis à la carte convertisseur (CC).

4).- La carte convertisseur compare le cryptogramme constitué par la clé de test cryptée par la clé de réseau $(TK)_{NK}$ avec ceux répertoriés dans la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ qui peut être soit une liste noire (black list) ou liste des valeurs non autorisées, soit une liste blanche (white list) ou liste des valeurs autorisées.

Un cryptogramme $(TK)_{NK}$ contenu dans une liste noire ou absente d'une liste blanche est invalide; cela signifie que la clé de réseau (NK) utilisée pour l'encryptage de la clé de test (TK) est refusée. Une signalisation adéquate, sous forme d'un message d'erreur par exemple, invite l'utilisateur à changer de carte et à recommencer l'opération de connexion.

Un cryptogramme $(TK)_{NK}$ appartenant à une liste blanche ou absente d'une liste noire est par contre accepté. Dans ce cas, la carte convertisseur (CC) génère aléatoirement une clé de session (SK) qu'elle crypte avec la clé publique (PK) précédemment reçue. La carte convertisseur transmet alors le clé encryptée $(SK)_{PK}$ à la carte de terminal (CT).

5).- La carte de terminal (CT) décrypte la clé de session (SK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de session (SK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le message résultant $(SK)_{NK}$ est transmis à la carte convertisseur (CC).

En général, la carte convertisseur (CC) vérifie l'authenticité des données de contrôle reçues au moyen d'une signature sécurisée provenant du centre de gestion.

Selon une variante de l'invention, la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée dans une mémoire du décodeur après réception, car elle peut constituer un fichier trop important pour être stocké dans la carte convertisseur (CC). La comparaison du cryptogramme $(TK)_{NK}$ avec ceux contenus dans la liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est effectuée par le décodeur (STB).

Selon une autre variante le centre de gestion transmet, au lieu de la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$, une adresse indiquant où cette liste peut être téléchargée via Internet. Cette variante nécessite, soit un décodeur (STB) disposant d'un canal de retour, soit un ordinateur possédant une connexion Internet. Le fichier sera alors soit stocké directement dans la mémoire du décodeur, soit transmis depuis l'ordinateur vers le décodeur.

Selon une autre variante la clé de test cryptée avec la clé de réseau $(TK)_{NK}$ est transmise de manière sécurisée par la carte convertisseur (CC) via le décodeur (STB) vers un serveur adéquat ou vers le centre de gestion où la liste $\{(TK)_{NK1},$

$(TK)_{NK2}$, $(TK)_{NK3}$ ...} est stockée. La vérification de la validité de la clé $(TK)_{NK}$ est donc effectuée en ligne et seul un message d'acceptation ou de refus, avec éventuellement une signature de la clé, sera alors retourné à la carte convertisseur (CC). L'avantage de cette variante est de décharger le décodeur de tâches qui peuvent devenir importantes surtout avec une liste dont la longueur ne peut que croître avec le nombre de réseaux domestiques installés.

REVENDICATIONS

1. Méthode de vérification de la validité d'une clé de réseau dans un réseau domestique numérique comprenant un décodeur (STB) de flux de données (DT) encryptées par des mots de contrôle (CW) qui sont eux-mêmes contenus dans des messages de contrôle (ECM) provenant d'un centre de gestion et un ou une pluralité d'appareils (TV1, TV2, PC) définissant un réseau domestique, ledit décodeur (STB) comportant un module de sécurité appelé carte convertisseur (CC) chargée de réencrypter les mots de contrôle (CW) avec une clé de session (SK) générée aléatoirement par ladite carte formant des messages de contrôle locaux (LECM), ledit réseau partageant une clé de réseau (NK) propre au dit réseau et stockée uniquement dans les modules de sécurité des appareils de visualisation (TV1, TV2, PC) appelés cartes de terminal (CT), la clé de session (SK) accompagnant lesdits messages de contrôle locaux (LECM) étant encryptée par la clé de réseau (NK) dans une des cartes de terminal (CT), caractérisée par les étapes suivantes:

- réception par la carte convertisseur (CC) d'une clé de test (TK) et de données de contrôle provenant du centre de gestion via le décodeur (STB),

- transmission de la clé de test (TK) via le réseau domestique vers une carte de terminal (CT) associée à l'un des appareils (TV1, TV2, PC) connectés au réseau,

- encryption par la carte de terminal (CT) de la clé de test (TK) avec la clé de réseau (NK) contenue dans ladite carte de terminal (CT),

- transmission de la clé de test (TK) encryptée vers la carte convertisseur (CC),

- comparaison de la clé de test (TK) encryptée avec les données de contrôle précédemment reçues,

- acceptation ou refus de transmettre des données à ce réseau domestique en fonction du résultat de la comparaison.

2. Méthode selon la revendication 1, caractérisée en ce que les données de contrôle consistent en une liste noire (black list) $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ contenant des cryptogrammes obtenus par l'encryption de la clé de test (TK) avec des clés de réseau invalides (NK1, NK2, NK3,...).

3. Méthode selon la revendication 1, caractérisée en ce que les données de contrôle consistent en une liste blanche (white list) $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ contenant des cryptogrammes $(TK)_{NK}$ obtenus par l'encryption de la clé de test (TK) avec des clés de réseau valides (NK1, NK2, NK3,...).

4. Méthode selon les revendications 1 à 3, caractérisée en ce qu'un cryptogramme $(TK)_{NK}$ absent de la liste noire ou présent dans liste blanche est accepté lors de la comparaison entraînant les étapes suivantes:

- génération aléatoire de la clé de session (SK),

- transmission de cette clé (SK) à la carte de terminal (CT) de manière sécurisée,

- encryption de la clé de session (SK) par la carte de terminal (CT) à l'aide de la clé de réseau (NK),

- transmission de la clé de session encryptée $(SK)_{NK}$ à la carte convertisseur (CC),

- encryption des mots de contrôle (CW) par la carte convertisseur (CC) à l'aide de ladite clé de session (SK)

- transmission de la clé de session encryptée $(SK)_{NK}$ et des mots de contrôle (CW) encryptés par la clé de session (SK) à la carte de terminal (CT) avec le flux de données (DT) encryptées par les mots de contrôle (CW).

5. Méthode selon la revendication 1 à 3, caractérisée en ce qu'un cryptogramme présent $(TK)_{NK}$ dans la liste noire ou absent de la liste blanche est refusé lors de la comparaison, une signalisation d'erreur invitant l'utilisateur à changer de carte de terminal (CT) est alors générée.

6. Méthode selon les revendication 1 à 5 caractérisée en ce que la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée dans une mémoire du décodeur après réception, la comparaison avec le cryptogramme $(TK)_{NK}$ s'effectue au niveau du décodeur (STB).

7. Méthode selon les revendications 1 à 5 caractérisée en ce que les données de contrôle consistent en une adresse indiquant où la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ peut être téléchargée via Internet au moyen du décodeur (STB)

ou d'un ordinateur (PC), ladite liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} ...\}$ est alors stockée dans la mémoire du décodeur (STB).

8. Méthode selon la revendication 1 caractérisée en ce que la carte convertisseur (CC) vérifie l'authenticité des données de contrôle au moyen d'une signature sécurisée provenant du centre de gestion.

9. Méthode selon la revendication 1 caractérisée en ce que les données de contrôle consistent en un message d'acceptation ou de refus du cryptogramme $(TK)_{NK}$, ledit cryptogramme étant préalablement transmis vers un centre de gestion par la carte convertisseur (CC) via le décodeur (STB), la liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} ...\}$ est stockée par le centre de gestion, la vérification de la validité du cryptogramme $(TK)_{NK}$ est effectuée en ligne.

ABRÉGÉ

Le but de la présente invention est de proposer une méthode de contrôle de la conformité d'une clé de réseau (NK). Cette méthode s'applique lors du transfert de données provenant d'une source à accès conditionnel vers un réseau domestique. Il s'agit de vérifier l'authenticité d'une clé de réseau (NK) par l'intermédiaire de données de contrôle pertinentes fournies par le centre de gestion en général sous forme d'une liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$.

Une vérification de la présence ou de l'absence d'un cryptogramme $(TK)_{NK}$ est effectuée selon la liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$. Le cryptogramme $(TK)_{NK}$ est constitué à partir d'une clé de test (TK) fournie par le centre de gestion encryptée par une clé de réseau (NK) d'un module de sécurité (CT) d'un appareil (TV1, TV2, PC) connecté au réseau.

Figure 2

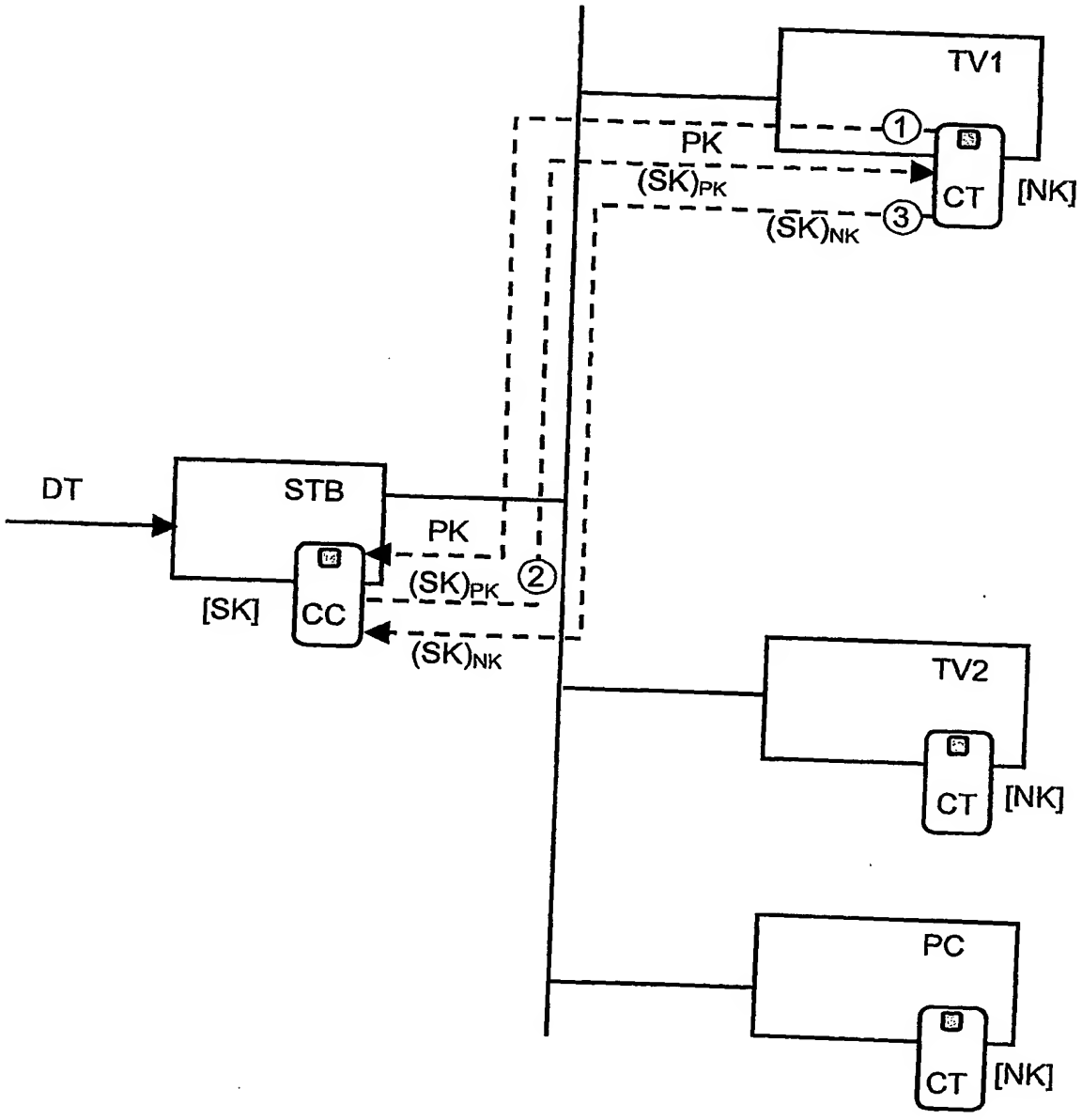

Fig. 1

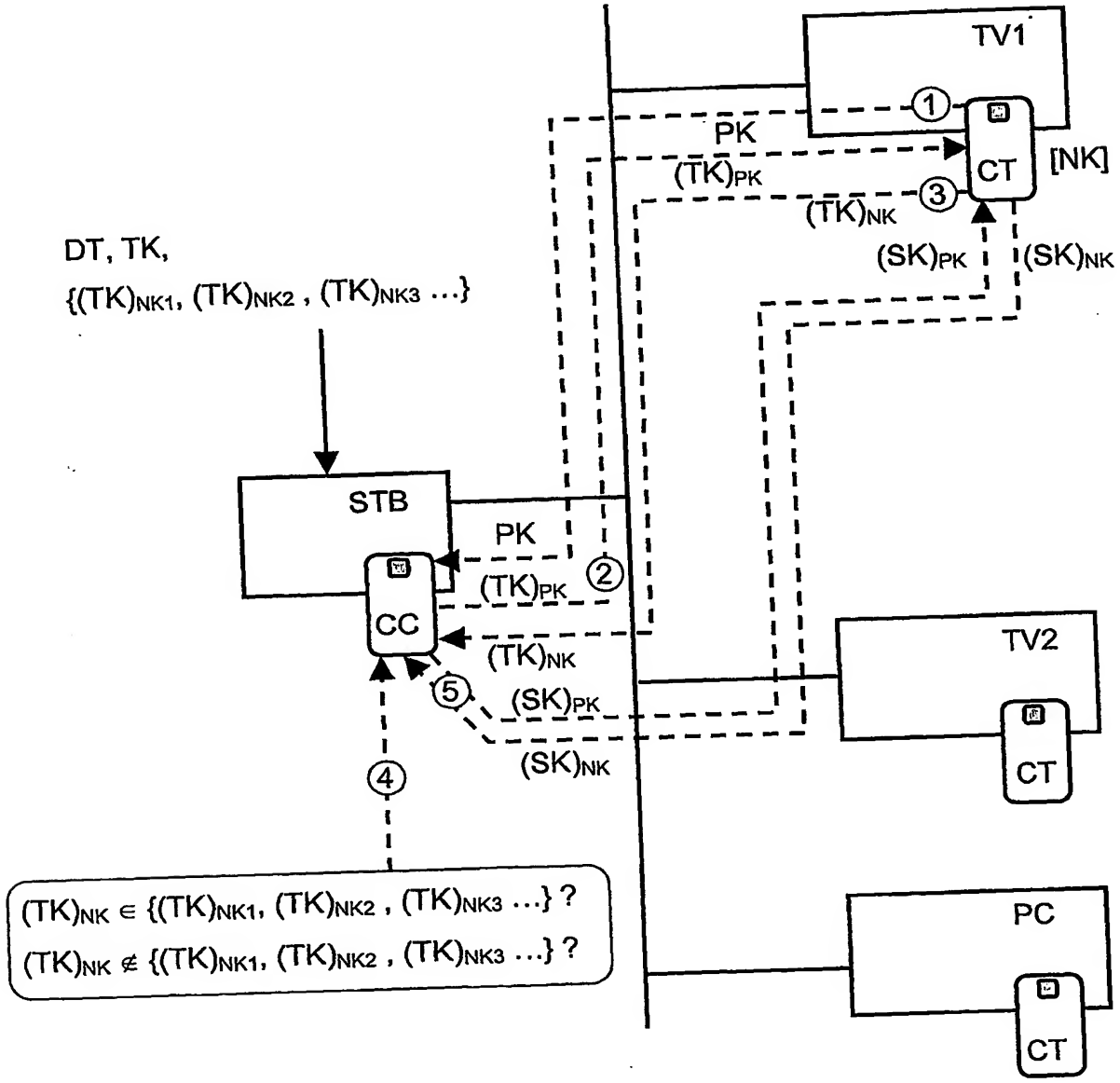

Fig. 2